대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2002년 제 56937 호
Application Number PATENT-2002-0056937

출 원 년 월 일 : 2002년 09월 18일
Date of Application SEP 18, 2002

출 원 인 : 학교법인 한국정보통신학원
Applicant(s) INFORMATION AND COMMUNICATIONS UNIVERSITY EDUCATION/

2002 년 10 월 01 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0003

【제출일자】 2002.09.18

【발명의 명칭】 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법

【발명의 영문명칭】 IDENTIFICATION SCHEME BASED ON THE BILINEAR DIFFIE-HELLMAN PROBLEM

【출원인】

【명칭】 학교법인 한국정보통신학원

【출원인코드】 2-1999-038195-0

【대리인】

【성명】 장성구

【대리인코드】 9-1998-000514-8

【포괄위임등록번호】 2000-005740-6

【대리인】

【성명】 김원준

【대리인코드】 9-1998-000104-8

【포괄위임등록번호】 2000-005743-8

【발명자】

【성명의 국문표기】 김명선

【성명의 영문표기】 KIM,Myung Sun

【주민등록번호】 700521-1478511

【우편번호】 305-348

【주소】 대전광역시 유성구 화암동 58-4

【국적】 KR

【발명자】

【성명의 국문표기】 김광조

【성명의 영문표기】 KIM,Kwang Jo

【주민등록번호】 560410-1347622

【우편번호】	305-348
【주소】	대전광역시 유성구 화암동 58-4
【국적】	KR
【심사청구】	청구
【조기공개】	신청
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구 , 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인 장성구 (인) 대리인 김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	2	면	2,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	5	항	269,000 원
【합계】	300,000 원		
【감면사유】	학교		
【감면후 수수료】	150,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 개인 식별 기법에 관한 것으로, 인터넷과 같은 사이버 공간의 비대면(非對面) 상황에서 증명자 자신의 비밀을 노출시키지 않으면서 검증자에게 자신의 신분을 확인하는 다양한 서비스에 요구된다. 인수분해의 어려움이나 이산대수 문제의 어려움에 기반을 두고 있는 기존의 방법은 수차례의 대화식 질의-응답 과정을 필요로 하며 안전성에 대한 증명이 직관적이지 못하다. 본 발명에서는 일방향 함수로 알려진 겹선형 디피-헬만 문제(Bilinear Diffie-Hellman Problem)에 기반한 식별 프로토콜을 설계하고 이것의 안전성에 대한 정량적 근거를 복잡도 이론에 근거한 암호학적 축소 방법을 사용하여 엄격하게 제시한다.

【대표도】

도 5

【명세서】

【발명의 명칭】

겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법

{IDENTIFICATION SCHEME BASED ON THE BILINEAR DIFFIE-HELLMAN PROBLEM}

【도면의 간단한 설명】

도 1은 일반적인 개인 식별 과정을 나타낸 순서도,

도 2는 본 발명에 따른 개인 식별 프로토콜 참가자들간의 상호작용 구성도,

도 3은 본 발명에 따른 개인 식별 방법의 전체 순서도,

도 4a 내지 도 4c는 도 2의 구성도에 기반하여 도 3의 개인 식별 방법의 세부 과정을 설명하기 위한 도면,

도 5는 본 발명에 따른 개인 식별 방법으로서, 도 3의 상세 메시지 계산 및 동작 과정을 나타낸 순서도.

<도면의 주요부분에 대한 부호의 설명>

100 : 증명자 200 : 검증자

300 : 시스템 관리자

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 네트워크상의 개인 식별 기법에 관한 것으로, 특히, 겹선형 디피-헬만 문제(Bilinear Diffie-Hellman Problem)를 이용하여 가상 공간에서 개인 식별 과정을 안

전하게 설계하는데 적합한 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법에 관한 것이다.

<10> 현재, 네트워크 환경의 꾸준한 발전과 더불어 기존의 오프-라인(off-line)에서만 국한되던 각종 서비스들이 인터넷을 통한 사이버 공간으로 확산되고 있는 추세이다. 이러한 사이버 공간의 가장 큰 장점중 하나는 언제 어디서나 네트워크를 통해 원격 비대면(非對面) 연결이 가능하다는 점이다. 그러나, 이러한 비대면성을 갖는 가상 공간에서는, 오프-라인 상에서처럼 상대방을 직접 확인할 수 없는 바, 정당한 사용자인지 아니면 정당한 사용자를 가장한 불법적인 사용자인지를 구별여야만 하는 근본적인 해결 과제가 존재한다.

<11> 일반적으로, '개인 식별 기술'은 사이버 공간을 포함한 대부분의 비대면 상황에서 암호학적 기술 요소들을 사용하여 이러한 문제들을 해결한다.

<12> 이하에서는, 이러한 개인 식별 기술의 보다 구체적인 내용을 도 1을 참조하여 설명하기로 한다.

<13> 도 1은, 전형적인 개인 식별 과정을 기술한 것으로서, 인터넷을 통한 사이버 은행거래를 대표적인 예로 들 수 있다.

<14> 인터넷을 통한 사이버 은행거래에서는, 공개키와 비밀키를 가진 공개키 암호시스템을 이용하는데, 통상, 비밀키는 그 소유자만이 인지하고 있으며, 공개키는 공개된다.

<15> 먼저, 비밀키를 소유한 것으로 예상되는 증명자 P가 검증자 V가 소유한 서비스를 요청한다. 이때, 증명자 P는 검증자 V의 어떠한 질의에 대하여 자신의 비밀을

누출시키기 않으면서 자신이 공개한 공개키에 대응하는 비밀키를 소유하고 있는 정당한 사용자라는 것을 증명하려고 한다. 동시에 검증자 V는 증명자 P의 공개된 정보만을 이용하여 증명자의 정당성을 검증하고자 한다.

<16> 가장 기본적인 개인 식별 방법은 사용자별로 특정한 아이디 정보와 사용자만이 알고 있는 패스워드 정보을 이용한 것으로서, 대부분의 유닉스 운영체제 하에서 이용되는 방법이다. 그러나, 이 방법은 자신의 비밀키, 즉, 증명자 P의 패스워드가 안전하지 않은 통신 채널을 통하여 전송될 때 제 3 자에게 노출될 가능성이 대단히 높아 불법적인 위장 공격이 가능하다는 문제가 있다.

<17> 한편, 정수론에 기반을 둔 공개키 암호 시스템을 이용하는 개인 식별 방법은 크게 두 가지로 분류될 수 있다. 첫 번째는 피아트(Fiat)와 샤미르(Shamir)에 의해 제안된 식별 기법으로 피아트-샤미르 기법이라 하며, 두 번째는 슈노르(Schnorr)에 의해서 제안된 슈노르 기법이다. 피아트-샤미르 기법은 정수의 소인수분해 문제의 어려움에 기반한 식별 방법이며, 슈노르 기법은 이산대수 문제의 어려움에 기반한 식별 방법이다.

<18> 먼저, 피아트-샤미르 방법 및 이 방법의 변형된 동작 원리는 다음과 같다.

<19> 신뢰할 수 있는 시스템 관리자는 충분히 큰 수 n값을 결정한다. 증명자 P는 n과 서로 소인 자신의 비밀키 a를 선택하여 $b=a^2 \bmod n$을 계산한다. 증명자 P는 b를 공개한다. 그리고, 증명자 P와 검증자 V 상호간에는 다음과 같은 프로토콜이 수 회 반복 실행된다.

<20> 가. 먼저, 증명자 P는 $r \in Z_n^*$인 임의의 r을 선택하고 $x=r^2$을 계산하여 x를 검증자 V에게 전송한다.

<21> 나. 검증자 V는 증명자 P에게 임의의 $e \in Z_n^*$을 선택하여 전송한다.

<22> 다. 증명자 P가 ε을 받으면 $y=r\cdot a^{\varepsilon} \bmod n$을 계산하여 전송한다.

<23> 라. 검증자 V는 $y^2=x\cdot b^{\varepsilon} \bmod n$인지 검사하여 참이면 증명자 P를 정당한 증명자로 받아들이고 거짓이면 위 프로토콜을 즉시 중단한다.

<24> 다음으로, 슈노르에 의해서 제안된 개인 식별 기법에 대해 기술하기로 한다.

<25> 여기서, p는 충분히 큰 소수이며, 법 p의 곱셈군의 법 p의 부분군을 이용한다. 이때 $p-1$은 q로 나누어진다. 또한, 임의의 한 원소 β가 선택되며 이것의 위수는 q이다. 그러면, 증명자 P의 비밀키 a가 $1 \le a \le q-1$의 범위에서 선택되어 $v=\beta^{-a} \bmod p$를 계산하여 공개키로 한다. 그 후 다음 프로토콜을 1회 실행한다. 여기서 $cert_p$는 증명자 P의 인증서이다.

<26> 가. 증명자 P가 인증서와 $x=\beta^{r} \bmod p$를 계산하여 검증자 V에게 전송한다.

<27> 나. 검증자 V는 임의의 $\varepsilon \in Z_q^*$를 선택하여 증명자 P에게 전송한다.

<28> 다. 증명자 P는 $y=a\varepsilon + r \bmod q$를 계산하여 검증자 V에게 전송한다.

<29> 라. 검증자 V는 $x=\beta^{y}\cdot v^{\varepsilon} \bmod p$인지 검사하여 참이면 P를 정당한 증명자로 받아들이고 거짓이면 즉시 프로토콜을 중단한다.

<30> 이상과 같이, 피아트-샤미르와 슈노르에 의한 각각의 개인 식별 기법을 간략히 설명하였다.

<31> 그런데, 이러한 기법들에서는 몇 가지 문제점들이 존재한다.

<32> 먼저, 피아트-샤미르 방법의 단점은 크게 두 가지이다. 첫째는 증명 과정이 복잡하다는 것이고, 둘째는 도 1에서 주어진 "신분 증명 요청" 단계를 수 회 반복해야만 한다는 것이다. 피아트-샤미르 기법의 증명은 대화식 영지식 증명이라는 복잡도 이론에 근거

하여 안전성을 증명하였으나, 증명 과정이 매우 복잡하여 직관적 이해를 주지 못한다. 또한, 피아트-샤미르 방법이 제안된 이후 몇 가지 방법이 제안되었으나 대부분 대화식 영지식 증명에 의해서 안전성 증명이 이루어지며, 샤우프에 의해서 수학적 이론에 근거한 증명이 주어지기는 하지만 인수분해 문제의 어려움에 기반을 두었다는 점에서 여전히 단점으로 남아있다.

<33> 슈노르 기법의 문제는 인증서와 관련된 것으로 인증서의 확인 및 철회 등은 이미 널리 알려진 바와 같이 운영상의 문제뿐 아니라 성능 저하에도 영향을 미친다. 슈노르 개인 식별 기법도 기본적 동작원리 측면에서 보면, 도 1의 방식으로 동작하며 기본적으로 계산 능력이 상대적으로 낮은 클라이언트와 이에 비해 상대적으로 계산 능력이 높은 서버와의 식별을 위한 방법으로 제안되었으며 최근에 이르러서야 대화식 영지식 증명으로 안전성이 분석되었다. 즉, 슈노르 기법은, 안전성과 간편성을 제공하고는 있으나 계산능력이 비대칭적인 환경에만 주안점을 두고, 서버 대 서버의 식별 같은 대칭적인 환경에 적용하기에는 여러 가지 어려움이 있는 것이다.

<34> 따라서, 직관적 이해를 주는 엄밀한 안전성 증명과 한 번만 수행해도 되는 간편성을 제공하고, 대칭적 환경에 적용이 용이한 네트워크상의 개인 식별 기술이 요망된다.

【발명이 이루고자 하는 기술적 과제】

<35> 본 발명은 상술한 요망에 의해 안출한 것으로, 사이버 공간의 비대면이라는 특수한 상황에서 겹선형 디피-헬만 문제를 이용하여 상대방이 정당한 사용자라는 것을 검증함으로써, 대칭적 계산 능력을 갖는 환경에 적합한 개인 식별 기법을 마련하도록 한 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법을 제공하는데 그 목적이 있다.

<36> 본 발명의 또 다른 목적은, 암호학적 축소 방법(암호학적으로 안전하다는 것을 현대 암호학계에서 가장 엄밀하게 증명하는 방법)을 사용하여 수동 공격자에 대해서 뿐만 아니라 능동 공격자에 대해서도 안전한 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법을 제공하는데 있다.

<37> 이러한 목적을 달성하기 위한 본 발명에 따른 개인 식별 방법은, 시스템관리자가 시스템 매개변수를 생성하는 단계; 증명자의 공개키 v와 비밀키 (a,b,c)쌍을 생성하는 단계; 증명자가 난수 (r_1,r_2,r_3)를 발생하여 자신이 비밀을 알고 있다는 증거 (x,Q)를 제시하는 단계; 검증자가 검증을 위해 자신이 생성한 임의의 수로 계산한 질의 R을 제시하는 단계; 제시된 질의에 대해서 응답 Y를 자신의 비밀키와 상술한 질의를 이용하여 계산한 후 검증자에게 제시하는 단계; 상기 검증자가 증명자가 제시한 최종값 Y, 증거 (x,Q) 및 공개키 v를 이용하여 증명자의 신분을 확인하는 단계를 포함하는 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법을 제공한다.

【발명의 구성 및 작용】

<38> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대해 상세히 설명한다.

<39> 도 2는 본 발명에 따른 개인 식별 기법의 개략적인 구성도를 도시한 것으로, 식별 프로토콜의 주 참여자는 증명자(100), 검증자(200) 및 시스템 관리자(300)를 포함하며, 이들 각각의 참여자는 컴퓨터 시스템으로 구현될 수 있다. 개인 식별 기법을 구성하는 각각의 참여자는 다음과 같은 기능을 수행한다.

<40> 먼저, 증명자(100)는 주어진 시스템 매개변수에 따라 공개키와 비밀키를 각각 생성하고, 생성된 공개키는 공개한 후 자신의 신분을 증명하기 위해서 공개키에 해당하는 비밀을 자신만이 안다는 것을 검증자(200)에게 제시하는 역할을 담당한다.

<41> 검증자(200)는 증명자(100)가 제시하는 값들의 유효성을 시스템 매개변수를 참조하여 검증하고, 증명자(100)가 제시하는 증거와 공개키 값을 근거로 하여 증명자(100)가 정당한 사용자인지를 판단하는 역할을 담당한다.

<42> 시스템 관리자(300)는 시스템 초기화시에만 동작하며, 자신이 생성한 시스템 매개변수들을 공지한다. 경우에 따라, 증명자(100)의 공개키와 비밀키 쌍을 생성하여 안전한 채널로 전송할 수 있다. 그러나 식별 과정에는 참여하지 않는다.

<43> 이하, 상술한 구성과 함께, 본 발명의 바람직한 실시예에 따른 네트워크 환경에서의 개인 식별 방법을 첨부한 도 3 내지 도 5를 참조하여 상세히 설명하기로 한다.

<44> 도 3에 도시한 바와 같이, 본 발명에 따른 개인 식별 기법은, 시스템 매개변수 생성 및 증명자(100) 공개키/비밀키 생성 과정(단계410), 증명자(100)와 검증자(200)간의 증거 제시, 질의 및 응답 과정(단계420, 단계430), 검증자(200)가 증명자(100)의 유효성을 판단하는 과정(단계440, 단계450)을 각각 포함하며, 이러한 과정에 의해 검증자(200)가 증명자(100)의 신분을 최종적으로 확인 할 수 있다.

<45> 먼저, 시스템 매개변수 생성 과정(단계410)은, 도 4a에 도시한 바와 같이, 증명자(100)와 검증자(200) 모두가 공유하는 시스템 매개변수들이 시스템 관리자(300)에 의해서 생성되어 공개되는 과정이다. 본 과정에서 임의의 순환군 G_1과 G_2가 생성되며, 이때

두 순환군의 위수는 m이다. 순환군 G_1상의 임의의 생성자 P를 생성한다. 끝으로, 두 순환군에 대한 겹선형 사상을 정의하고 변형된 겹선형 사상 $\hat{e}: G_1 \times G_1 \mapsto G_2$ 를 생성한다.

<46> 다음으로, 증거 제시, 질의 및 응답 과정(단계420, 단계430)은, 도 4b에 도시한 바와 같이, 시스템 관리자(300)가 공개한 시스템 매개변수에 기반하여 증명자(100)가 임의의 난수를 생성하여 증거를 제시하는 단계, 검증자(200)가 증명자(100)에게 질의 내용을 전송하는 단계, 증명자(100)가 자신의 비밀키와 전송된 질의 내용을 이용하여 응답을 계산한 후 이를 검증자(200)에게 전송하는 단계로 이루어진다.

<47> 그리고, 유효성 판단 과정(단계440, 단계450)은, 도 4c에 도시한 바와 같이, 검증자(200)가 자신이 생성한 질의와 증명자(100)의 비밀키에 대응하는 공개키 값을 이용하여 증명자(100)가 정당한 사용자인지 검증하는 과정이다. 본 과정에서 참 값을 얻으면 증명자(100)는 정당한 사용자로 판명되며, 거짓이면 즉시 식별 프로토콜 수행을 중단한다.

<48> 이때, 본 발명의 개인 식별 기법의 안전성은 크립토2001 학회에서 보네-프랭크린(Boneh-Franklin)에 의해서 제안된 겹선형 디피-헬만 문제의 어려움을 기반으로 하여 구성됨을 특징으로 한다. 시스템 관리자(300)는 타원곡선 상의 점들의 군과 유한체를 생성하고 이 두 순환군 간을 사상하는 변형 겹선형 사상을 생성한다. 이 값들은 공개되어 증명자(100)와 검증자(200) 모두에 의해서 이용되도록 한다.

<49> 한편, 본 발명의 주요 특징인 도 3에 예시된 개인 식별 과정의 흐름을 도 5의 흐름도를 참조하여 보다 상세히 설명된다.

<50> 먼저, 단계(510)에서는, 시스템 매개변수를 도 4a에 나타나는 것처럼 시스템 관리자에 의해서 위수가 m인 타원곡선상의 점들의 군 G_1과 , 역시 위수가 m인 유한체 G_2를 생성하고 변형 겹선형 사상을 정의한다. 이는 다음 수학식 1과 같이 표현될 수 있다.

<51> [수학식 1]

<52> $\hat{e}: G_1 \times G_1 \mapsto G_2$

<53> 그 다음 단계(520)에서, 상술한 시스템 매개변수를 이용하여 증명자(100) 또는 시스템 관리자(300)는 증명자(100)의 공개키와 비밀키 쌍을 생성한다. 먼저 Z_m^*에 속하는 임의의 값들, $<a,b,c>$ 를 비밀키로 선택하고, 다음 수학식 2에 의해서 공개키 v를 지정한다.

<54> [수학식 2]

<55> $v=\hat{e}(P, P)^{abc}$

<56> 이렇게 하여 계산된 공개키는 증명자(100)나 시스템 관리자(300)에 의해서 공개되며, 비밀키는 증명자(100)가 안전하게 보관한다. 그러므로, 검증자(200)는 언제든지 증명자(100)의 공개키에 접근할 수 있다.

<57> 그리고, 단계(530)에서는, 서비스에 접속하기 원하는 증명자(100)가 하기 수학식 3을 기반으로 증거를 생성하여 검증자(200)에게 제시한다. 이때, 수학식 3을 계산하기 위해 증명자(100)는 먼저 임의의 값 $r_1, r_2, r_3 \in Z_m^*$을 선택한다.

<58> [수학식 3]

<59> $x=\hat{e}(P, P)^{r_1 r_2 r_3}$, $Q=r_1 r_2 r_3 P$

<60> 이후, 이러한 수학식 3에 의해서 계산된 두 값 (x,Q) 를 검증자(200)에게 전송한다. 즉, 단계(530)에서와 같이, 본 발명은 하나의 증거 대신 두값(x,G), 즉, 제 1 증거와 제 2 증거를 동시에 계산하여 검증자(200)에게 전송함으로써, 증명자(100)가 자신의 증거를 계산할 때, 증명자(100)가 생성한 난수의 위변조를 방지할 수 있도록 구현한 것이다.

<61> 그 다음 단계(540)에서, 검증자(200)는 증명자(100)의 증거로서 (x,Q)을 받으면, 역시 난수 $\omega \in Z_m^*$을 생성하여 질의를 계산하고 이를 증명자(100)에게 전송한다. 이러한 질의 R은 다음 수학식 4와 같이 표현될 수 있다.

<62> [수학식 4]

<63> $$R=\omega P$$

<64> 이때, 본 발명은, 난수 자체를 전송하는 대신, 단계(540)에서 생성된 난수를 선택하여 순환국 GI에 속하는 값을 변형하여 전송함으로써 검증자(200)가 증명자(100)에게 질의를 보낼 때 질의 내용의 위변조를 방지하는 것을 특징으로 한다.

<65> 그 다음 단계(550)에서, 증명자(100)는 자신이 생성한 난수와 검증자(200)에게서 받은 질의를 사용하여 다음 수학식 5에 나타난 바와 같은 중간값을 먼저 계산한다.

<66> [수학식 5]

<67> $$S=r_1 r_2 r_3 R$$

<68> 이러한 중간값 계산은 후술하는 응답값의 위변조를 방지하기 위함이다.

<69> 이러한 중간값을 계산한 후, 증명자(100)는 검증자(200)에게 제시할 응답을 계산하고, 계산된 응답을 검증자(200)에게 전송한다. 이러한 응답 Y는 다음 수학식 6과 같이 표현될 수 있다.

<70> [수학식 6]

<71> $$Y=abcP+(a+b+c)S$$

<72> 이때, 본 발명에서는, 이러한 응답값 계산시 연산의 효율성을 위하여 타원곡선상의 2회 스칼라 곱셈($abcP$와 $(a+b+c)S$)과 1회 덧셈($abcP+(a+b+c)S$)만을 필요로 하는 것을 특징으로 한다.

<73> 단계(560)에서 검증자(200)가 응답을 받으면, 검증자(200)는 상기한 단계(550)에서 얻은 값과 공개키를 사용하여 증명자(100)의 정당성 여부를 검증한 후 단계(570)에서와 같이 검증 결과를 통보한다.

<74> 먼저, 단계(560)에서 증명자(100)의 정당성은 다음 수학식 7과 같은 증거 유효성 결정에 의해 검증될 수 있다.

<75> [수학식 7]

<76> $$x=\hat{e}(P,Q)$$

<77> 만일, 수학식 7의 값이 유효하다면 다음 수학식 8을 계산하고, 유효하지 않다면 단계(570)를 수행하여 증명자(100)에게 무효한 사용자임을 알린다.

<78> [수학식 8]

<79> $$\hat{e}(Y,P)=v\ \hat{e}(aP+bP+cP,\ Q)^{\circ}$$

<80> 수학식 8의 결과가 참인 것으로 검증되면 검증자(200)는 단계(570)를 수행하여 증명자(100)에게 서비스에 접근할 수 있다는 것을 통보하며(단계470), 거짓인 경우에는 단계(570)를 수행하여 증명자(100)가 잘못된 사용자임을 알리고 서비스 접근을 거부한다(단계460).

<81> 이상과 같이, 상술한 본 발명의 개인 식별 기법을 이용하면 증명자는 자신의 비밀정보를 검증자에게 알리지 않고도 자신이 올바른 사용자라는 것을 3번의 상호 대화식 작용을 이용하여 효율적으로 증명할 수 있다.

<82> 상술한 내용 중 시스템 관리자가 증명자에게 공개키와 비밀키를 생성하여 제공할 수도 있다. 그러나, 본 발명은 서로의 성능이 대칭적인 경우를 주요 대상으로 하였다는 것을 감안한 바, 증명자 스스로 자신의 공개키와 비밀키를 생성할 충분한 능력을 보유한 것으로 볼 수 있다. 즉, 시스템 관리자가 공개키와 비밀키 쌍을 생성하여 제공하는 것은 선택사항이다.

【발명의 효과】

<83> 본 발명은 겹선형 디피-헬만 문제에 기반한 안전한 식별 방법이 구성될 수 있음을 보여주고 있다. 동시에 안전성 증명이 수학적 모델링을 통하여 매우 엄밀하게 제시되고 있다. 특히, 기반 문제가 블랙박스 시뮬레이터를 갖는지 증명되지 않은 경우에 대화식 영지식 증명으로 프로토콜의 안전성을 증명할 수 없었으나, 본 발명에서는 위와 같은 선행 조건에 관계없이 안전성 증명이 영지식 상호증명만큼 엄밀하게 이루어질 수 있음을 보였다.

<84> 특히, 개인 사용자 컴퓨터의 계산 능력이 서버에 대응할 수 있을 정도로 급변하고 있는 시대에 즈음하여, 서버 대 서버의 상호 식별뿐만 아니라 개인 대 서버의 식별에도 적용할 수 있다.

<85> 겹선형 사상은 테이트 쌍이나 베일 쌍을 타원곡선 상에서 구현하여 사용하였다. 이때, 테이트 쌍이나 베일 쌍의 계산이 상대적으로 복잡하여 연산의 비효율성이 지적되었다. 그러나, 현재 암호학자들의 지속적인 연구로 인하여 연산 시간 개선이 꾸준히 이루어지고 있으며 최근에는 계산량을 줄이는 알고리즘의 연구에 힘입어 테이트 쌍이나 베일 쌍의 연산도 매우 효율적으로 계산되고 있다. 그러므로, 본 발명은 서버 대 서버 같은 대칭적 계산 능력을 요구하는 상황뿐 아니라 클라이언트 대 서버같은 비대칭적인 상황에도 적용할 수 있다.

<86> 이상, 본 발명을 실시예에 근거하여 구체적으로 설명하였지만, 본 발명은 이러한 실시예에 한정되는 것이 아니라, 하기 특허청구범위의 요지를 벗어나지 않는 범위내에서 여러 가지 변형이 가능한 것을 물론이다.

【특허청구범위】

【청구항 1】

증명자, 검증자 및 시스템 관리자로 구성되는 네트워크 환경에서의 개인 식별 방법에 있어서,

상기 시스템 관리자를 통해 시스템 매개변수 $<G_1, G_2, P, \hat{e}>$를 생성하는 제 1 단계와;

상기 증명자 또는 상기 시스템 관리자를 통해 비밀키 $<a,b,c>$ 와 공개키 v를 생성하는 제 2 단계와;

상기 증명자를 통해 난수 $(r_1, r_2, r_3) \in Z_m^*$을 생성하여 증거(x,Q)를 계산한 후, 그 결과를 상기 검증자로 전송하는 제 3 단계;

상기 검증자에서 상기 증거 계산 결과에 대한 난수 ω를 생성하고, 질의 R을 계산하여 상기 증명자로 전송하는 제 4 단계;

상기 증명자에서 상기 질의에 대한 중간값 S와 응답 Y를 계산하여 상기 검증자로 전송하는 제 5 단계;

상기 시스템 매개변수, 상기 증명자의 공개키, 상기 증명자의 증거, 상기 검증자의 난수 중 적어도 하나 이상의 데이터를 이용하여 상기 증거의 유효성과 상기 증명자의 정당성을 검증하는 제 6 단계를 포함하는 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법.

【청구항 2】

제 1 항에 있어서,

상기 제 3 단계는, 제 1 증거($x=\hat{e}(P, P)^{r_1 r_2 r_3}$) 및 제 2 증거($Q=r_1 r_2 r_3 P$)를 동시에 계산하여 검증자로 전송하는 단계인 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법.

【청구항 3】

제 1 항에 있어서,

상기 제 4 단계는, 생성된 난수를 선택하여 순환군 G_1에 속하는 값을 변형하여 전송하는 단계인 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법.

【청구항 4】

제 1 항에 있어서,

상기 제 5 단계는, 상기 증명자를 통해 증거로 제시한 값을 포함하는 중간값을 사용하며, 타원곡선상의 2회 스칼라 곱셈(*abcP*와 *(a+b+c)S*)과 1회 덧셈(*abcP+(a+b+c)S*)만을 필요로 하는 단계인 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법.

【청구항 5】

제 1 항에 있어서,

상기 제 6 단계는,

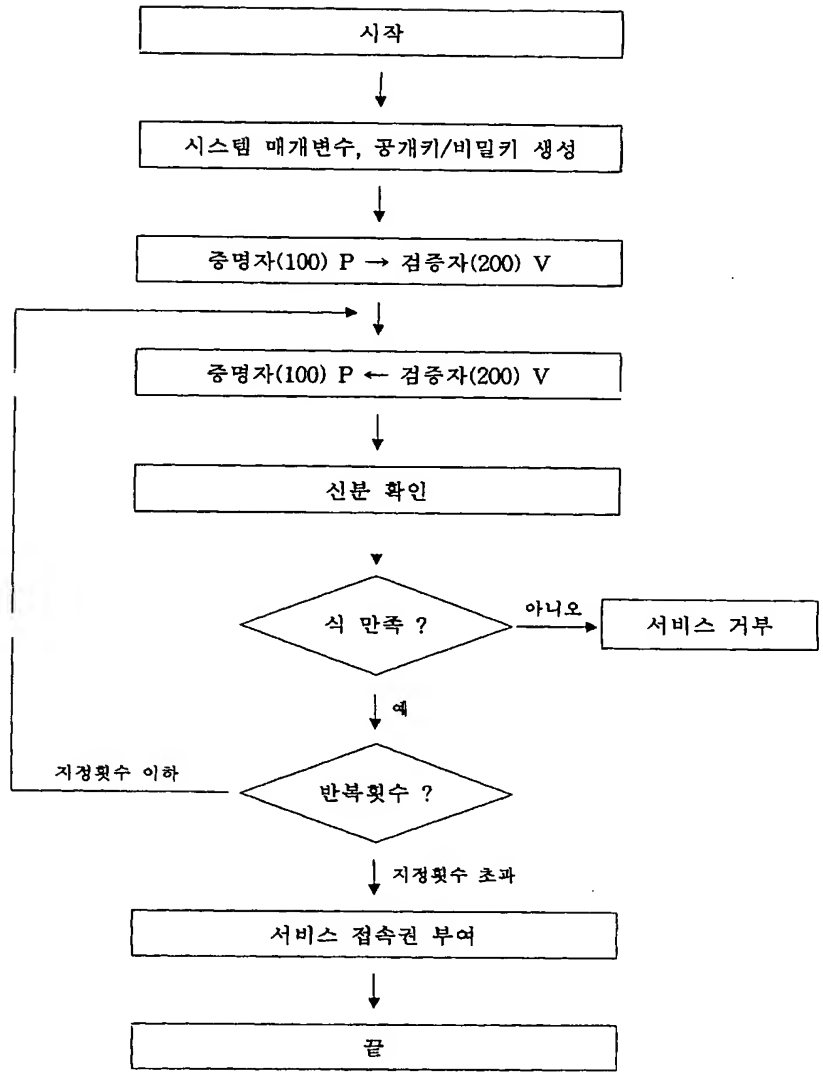
하기 수학식

$$
\begin{aligned}
\hat{e}(Y,P) &= \hat{e}(abcP+(a+b+c)S,P) \\
&= \hat{e}(abcP+(a+b+c)r_1r_2r_3R,P) \\
&= \hat{e}(abcP+(a+b+c)r_1r_2r_3\omega P,P) \\
&= \hat{e}((abc+(a+b+c)r_1r_2r_3\omega)P,P) \\
&= \hat{e}(P,P)^{abc+(a+b+c)r_1r_2r_3\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,P)^{(a+b+c)r_1r_2r_3\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,r_1r_2r_3P)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,Q)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}((a+b+c),PQ)^{\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(aP+bP+cP,Q)^{\omega} \\
&= v \cdot \hat{e}(aP+bP+cP,Q)^{\omega}
\end{aligned}
$$

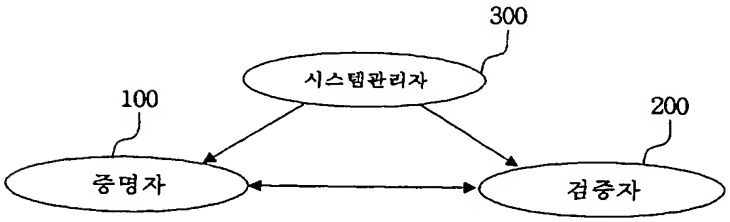
를 만족하는지를 검증하는 단계인 것을 특징으로 하는 겹선형 디피-헬만 문제에 기반한 네트워크 환경에서의 개인 식별 방법.

【도면】

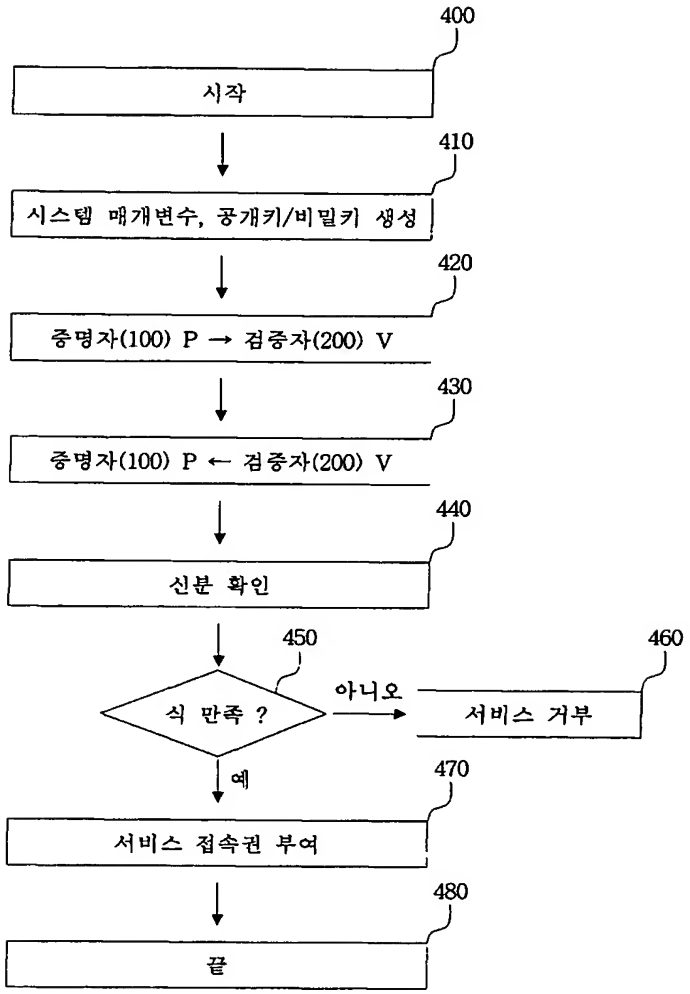
【도 1】


시작
시스템 매개변수, 공개키/비밀키 생성
증명자(100) P → 검증자(200) V
증명자(100) P ← 검증자(200) V
신분 확인
식 만족 ?
아니오
서비스 거부
예
지정횟수 이하
반복횟수 ?
지정횟수 초과
서비스 접속권 부여
끝

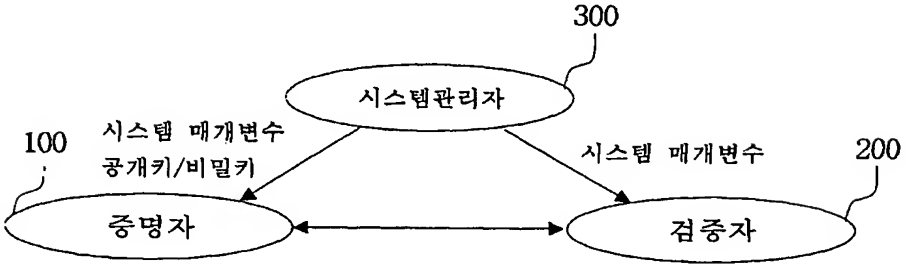
【도 2】


300
시스템관리자
100
200
증명자
검증자

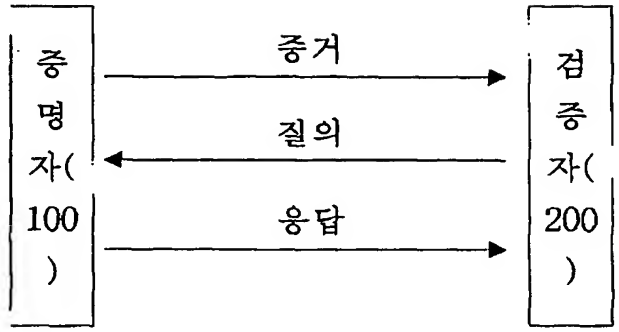
【도 3】


400
시작
410
시스템 매개변수, 공개키/비밀키 생성
420
증명자(100) P → 검증자(200) V
430
증명자(100) P ← 검증자(200) V
440
신분 확인
450
식 만족 ?
아니오
460
서비스 거부
예
470
서비스 접속권 부여
480
끝

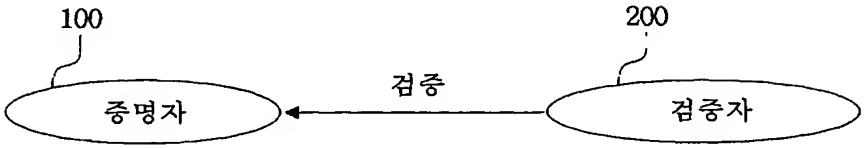
【도 4a】


300
시스템관리자
100
시스템 매개변수
공개키/비밀키
시스템 매개변수
200
증명자
검증자

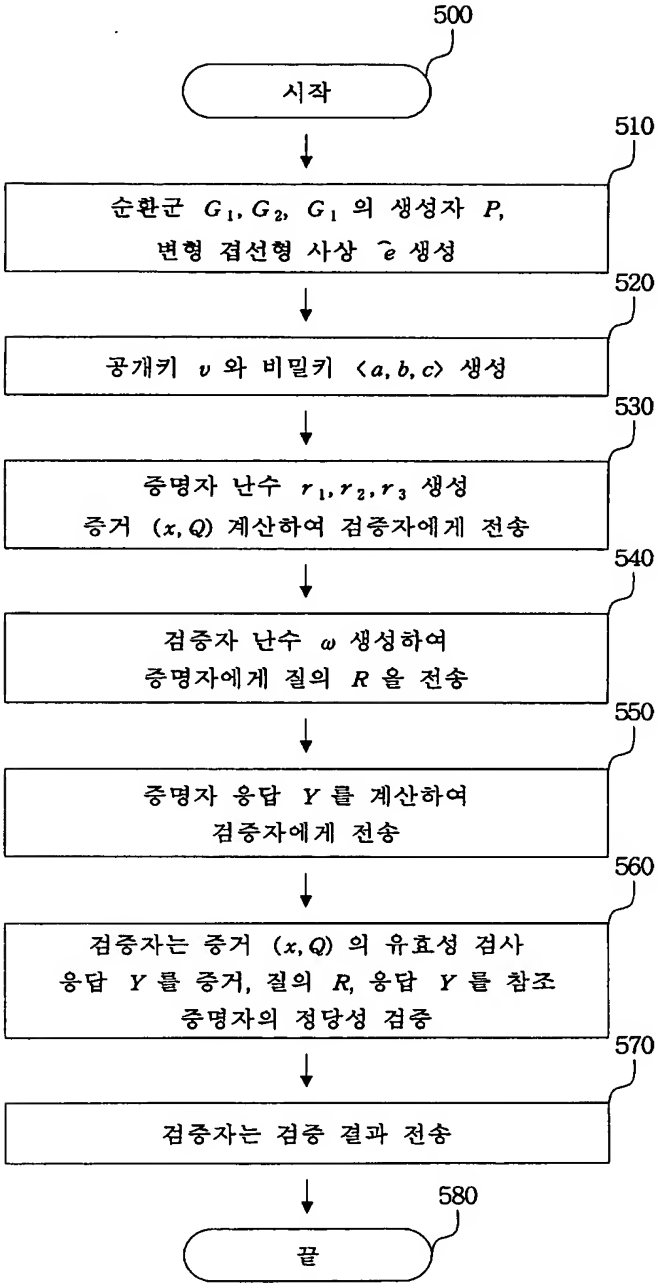
【도 4b】



【도 4c】



【도 5】


500
시작
510
순환군 G_1, G_2, G_1 의 생성자 P,
변형 겹선형 사상 $\hat{e}$ 생성
520
공개키 v 와 비밀키 $\langle a, b, c \rangle$ 생성
530
증명자 난수 r_1, r_2, r_3 생성
증거 (x, Q) 계산하여 검증자에게 전송
540
검증자 난수 ω 생성하여
증명자에게 질의 R 을 전송
550
증명자 응답 Y 를 계산하여
검증자에게 전송
560
검증자는 증거 (x, Q) 의 유효성 검사
응답 Y 를 증거, 질의 R, 응답 Y 를 참조
증명자의 정당성 검증
570
검증자는 검증 결과 전송
580
끝